# DEPARTMENT OF STATE

# PRIVACY IMPACT ASSESSMENT
**for**
*Electronic Telephone Directory (e*Phone)*
(Updated May 2008)

**Conducted by:**
**Bureau of Administration**
**Information Sharing Services**
**Office of Programs and Services**

## A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION

**1) Does this system collect, maintain or disseminate personally identifiable information (PII) about individual members of the public? If the above answer is yes, please complete the survey in its entirety. If no, complete the certification page and submit the PIA to the following e-mail address: pia@state.gov.**

**YES X NO__**

**2) Does a Privacy Act system of records already exist?**

**YES X NO__**

If yes, please provide the following**:**

**System Name: Electronic Telephone Directory (e*Phone)**

**Number: State-40**

**3) What is the purpose of the system/application?**

E*Phone is an online, browser-based employee directory for government employees and contractors. An employee with an authorized e*Phone directory account can access and update their public and private information.

**4) What legal authority authorizes the purchase or development of this system/application?**

Homeland Security Presidential Directive 12.

## B. DATA IN THE SYSTEM:

**1) What categories of individuals are covered in the system?**

Department employees and contractors.

**2) What are the sources of the information in the system?**

**a. Who/what is the source of the information?**

Users have their names entered into the e*Phone database by a system administrator; they then maintain the information.

**b. What type of information is collected from the source of the information?**

Name, password, date/time of access, date of last password change, date of last user record update, gender, marital status, employee type, supervisor name, building location, room number, state e-mail address, office phone number, 5-digit extension (if one exists), home phone number, employee type (Civil Service, Foreign Service), international voice gateway route exchange number and extension, office/post symbol, office/post description, cell phone, pager number, home address, public remarks, and private remarks. Users may also add name, home phone, work phone and relationship to provide contacts for users with executive access (supervisors, bureau executives, and telephone operators). The contacts list is only accessible to executive access users.

**3) Accuracy, Timeliness, and Reliability**

**a. How will data collected from sources other than DOS records be verified for accuracy?**

Office phone numbers are retrieved from the Foreign Affairs Directory Service. All other data is input by the individual users. No data comes from non-DOS sources.

**b. How will data be checked for completeness?**

Correctness is the responsibility of the users.

**c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

Data currency is the responsibility of the users; supervisors may encourage currency.

## D. INTENDED USE OF THE DATA:

**1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?**

Yes. In an increasingly collaborative workplace, users are motivated to maintain contact with Department users worldwide in support of the wide range of strategic goals. The system further serves the Department community by establishing a system of emergency contacts.

**2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?**

Neither data derivation nor aggregation are involved in the application.

**3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?**

No members of the public will have access to this system and data analysis is not the function of the application. However, emergency management is greatly facilitated by the application.

**4) Will the new data be placed in the individual's record?**

The new user name and phone number are entered by the system administrators of the application; all other data is entered by the users. User names and phone numbers are typically found in Department Human Resource records.

5) **How will the new data be verified for relevance and accuracy?**

Data accuracy and relevance is the duty of the users.

6) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Searches involve the employee name, room, building, office phone, agency, office/post description and/or office post symbol in any combination.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

System administrators have access to reports, including:

- Alphabetical Domestic Employees
- Alphabetical Overseas Employees
- Alphabetical Domestic and Overseas Employees
- Employee and Emergency Contacts (by Org Code, Employee Type or Alphabetical)
- New/Changed Employees (by Org Code or Alphabetical)
- Alphabetical Separated Employees
- User Activity (data modification history)
- User Access
- Alphabetical Bureau Executives (assigned views of employee)

## E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The application operates at Main State and a spare is maintained in the Department's Information Management Center.

2) **What are the retention periods of data in this system?**

Official personnel records are maintained by HR.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Not applicable.

4) **Is the system using technologies in ways that the DOS has not previously**

**employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**

Not applicable.

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

Typical user data includes the time and date of log-on, the date of the last change to the password, and the date of the last update to user records.

Upon log-on, e*Phone sends an e-mail to the user to ensure that this person is the one actually using the application.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

There are no current plans to modify the system; should such modification occur, the concern for Privacy Act protections will continue.

8) **Are there forms associated with the system? YES X NO**

**If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?**

Form DS-4073, "Access to e*Phone for E&L Statements," is used in the Charleston Financial Management Center for Earnings and Leave Pay Center Administration. It contains language warning that the E&L employee will be accessing and printing information about colleagues, limiting access levels to direct-hire American employees only and stating that maintaining password privacy is the employee's duty. Additionally, it states that all information is protected by the Privacy Act.

Form DS-4072, "Bureau Level Access to e*Phone," is used to establish bureau-level access. It contains language warning that protecting the privacy of these records is of utmost importance. It is signed by the requestor, that employee's supervisor, and the executive director or administrative officer.

During the user log-in process, there is a "Terms & Conditions of Use" that allow system administrators to regularly monitor usage and ensure proper performance of applicable security features and procedures. Such agreement is a condition of use. It also provides a statement that the Privacy Act data in the application will not be disclosed except in accordance with application policies.

## F. ACCESS TO DATA

**1) Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?**

- Cleared Department of State government employees.
- Cleared Department of State contractors, including locally hired personnel.
- Cleared Department of State operations & maintenance personnel (both employees and contractors).
- Cleared Department of State IT security examiners.
- Cleared personnel from other agencies in D.C. and at posts worldwide.
- Office of the Inspector General auditors.
- General Accounting Office auditors.

**2) What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access is granted to employees immediately upon being hired and to contractors upon request. The e*Phone web site contains a wealth of information about its operation and use in the Frequently Asked Questions area. The criteria, procedures and controls are documented there. Responsibilities are documented in the "Terms and Conditions of Use" statement on the front page of the site.

**3) Will users have access to all data on the system or will the user's access be restricted? Explain.**

There are five categories of e*Phone users:

- General employees
- Supervisors
- Bureau executives
- Telephone operators
- System administrative personnel

When general employees log in, they can only see their own records. They can look up information regarding other employees' agency, office or post, and office phone number without logging in.

Supervisors can see the records of the people they supervise. This facilitates the supervisor being able to act in an emergency situation and make contacts aware of the issue. Likewise, bureau executives and telephone operators can see the records of people in their organization for the same purpose.

System administrative personnel not only can see but back up and restore data in e*Phone.

All users are under the same Rules of Behavior.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)**

There are several levels of protection in e*Phone. The first is access to OpenNet itself. Second is the system password, which meets the Department standards for length and variation of characters. The Secured Sockets Layer (SSL) protocol protects against user passwords being intercepted; passwords are also stored in the database in hashed format. The Department rules for password formation guard against someone guessing a password, and if someone fails to log in five times, the user ID is deactivated. Also, as previously stated, log-ins of users and authorized others accessing the account are documented by e-mail.

The security settings of the system are inspected annually, monitored, and reported on iPost. A full certification and accreditation with independent verification and validation is conducted every three years prior to re-authorization to operate. The last such re-authorization occurred in August 2007.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

Yes to all.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The Bureau of Administration's Global Publishing Solutions program provides information to the e*Phone user. The Office of Enterprise Network Management's Universal Trouble Ticket system does likewise, and a number of OpenNet Intranet links are also provided on the site.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**

No.

8) **Who is responsible for assuring proper use of the SHARED data?**

Not applicable.